Claims

1. A storage-medium rental system, comprising:

a rental-shop apparatus that generates right information relating to a right to use digital work held by a portable storage medium, and securely writes the generated right information to a portable semiconductor memory; and

a playback apparatus that securely reads the right information from the semiconductor memory, and judges whether the digital work held by the storage medium is allowed to be used, based on the read right information, and when judging affirmatively, obtains the digital work from the storage medium and plays back the obtained digital work.

2. A storage-medium rental system in which a rental agent provides, to a user, a portable storage medium holding digital work whose right of use is rented from the rental agent to the user, comprising:

the portable storage medium that holds the digital work by storing therein digital content data representing the digital work;

a portable semiconductor memory that has an area for securely storing information;

a rental-shop apparatus that, when the rental agent provides the storage medium to the user, generates right information relating to a right to use the digital work held

by the storage medium, and securely writes the generated right information into the area of the semiconductor memory; and

a playback apparatus that, upon receipt of an instruction from the user to play back the digital work, securely reads the right information from the area of the semiconductor memory, and judges whether the digital work is allowed to be used, based on the read right information, and when judging affirmatively, reads the digital content data from the storage medium and plays back the digital work based on the read digital content data.

3. A rental-shop apparatus that manages rental, from a rental agent to a user, of a right to use digital work held by a portable storage medium, comprising:

an obtaining unit operable to obtain medium identification information identifying the storage medium;

a generation unit operable to generate right information relating to the right to use the digital work, based on the obtained medium identification information; and

a writing unit operable to securely write the generated right information into an area of a portable semiconductor memory.

4. The rental-shop apparatus of Claim 3,

wherein the writing unit writes the right information

into the area of the semiconductor memory, upon receipt of a payment for rental of the right to use the digital work from the rental agent to the user.

5. The rental-shop apparatus of Claim 4,

wherein the storage medium holds the digital work by storing therein digital content data that has been generated by encrypting the digital work using an encryption key,

the generation unit prestores a decryption key corresponding to the encryption key, in correspondence with the medium identification information, and reads the decryption key corresponding to the obtained medium identification information, and generates the right information including the read decryption key, and

the writing unit writes the right information including the decryption key, into the area of the semiconductor memory.

6. The rental-shop apparatus of Claim 4,

wherein the generation unit generates the right information including playback-limiting information showing a limitation to be imposed on playback of the digital work, based on the obtained medium identification information, and

the writing unit writes the right information including the playback-limiting information, into the area of the semiconductor memory.

7. The rental-shop apparatus of Claim 6,

wherein the generation unit generates the right information including, as the playback-limiting information, a rental-use time limit indicating a time limit until when the rental agent allows the user to use the digital work, and

the writing unit writes the right information including the rental-use time limit as the playback-limiting information, into the area of the semiconductor memory.

8. The rental-shop apparatus of Claim 6,

wherein the generation unit generates the right information including, as the playback-limiting information, a rental-use period during which the rental agent allows the user to use the digital work, the rental-use period starting from a time at which the user firstly plays back the digital work, and

the writing unit writes the right information including the rental-use period as the playback-limiting information, into the area of the semiconductor memory.

9. The rental-shop apparatus of Claim 6,

wherein the generation unit generates the right information including, as the playback-limiting information,

a number of times the user is allowed to play back the digital work, and

the writing unit writes the right information including the number of times the user is allowed to use the digital work as the playback-limiting information, into the area of the semiconductor memory.

10. The rental-shop apparatus of Claim 4,

wherein the generation unit generates the right information including the obtained medium identification information, and

the writing unit writes the right information including the medium identification information, into the area of the semiconductor memory.

11. The rental-shop apparatus of Claim 10,

wherein the storage medium holds the digital work by storing therein digital content data that has been generated by encrypting the digital work using a content key,

the semiconductor memory prestores, in the area, a device key unique to the semiconductor memory,

the generation unit stores, in correspondence with the medium identification information, an encrypted content key that has been generated by encrypting the content key using the device key, and reads the encrypted content key

corresponding to the obtained medium identification information, and generates the right information including the read encrypted content key, and

the writing unit writes the right information including the encrypted content key, into the area of the semiconductor memory.

12. The rental-shop apparatus of Claim 10,

wherein the storage medium holds the digital work by storing therein digital content data that has been generated by encrypting the digital work using a content key, and further stores a disc key unique to the storage medium,

the generation unit stores, in correspondence with the medium identification information, an encrypted content key that has been generated by encrypting the content key using the disc key, and reads the encrypted content key corresponding to the obtained medium identification information, and generates the right information including the read encrypted content key, and

the writing unit writes the right information including the encrypted content key, into the area of the semiconductor memory.

13. The rental-shop apparatus of Claim 4, further comprising

an authentication unit operable to perform mutual authentication with the semiconductor memory,

wherein the writing unit writes the right information only when the mutual authentication is successful.

14. The rental-shop apparatus of Claim 4,

wherein the area of the semiconductor memory includes a plurality of application areas being provided in one-to-one correspondence with a plurality of application functions, each application area being provided for securely storing information for the corresponding application function,

one of the plurality of application functions is a rental function of renting the storage medium for use in a storage-medium rental system, and the application area corresponding to the rental function is used to store the right information, and

the writing unit writes the generated right information into the corresponding application area included in the area of the semiconductor memory.

15. The rental-shop apparatus of Claim 14,

wherein another one of the plurality of application functions is a membership card function of identifying a member of a rental shop, and the application area corresponding to the membership card function is used to store a member number

that identifies the user, and

the rental-shop apparatus further comprises:

a member number generation unit operable to generate a member number identifying the user as a member of the rental shop; and

a member number registration unit operable to write the generated member number into the application area corresponding to the membership card function.

16. The rental-shop apparatus of Claim 15,

wherein another one of the plurality of application functions is a bonus provision function of providing, from the rental agent to the user, point information showing points as a bonus in accordance with use of the storage medium, and the application area corresponding to the bonus provision function is used to store point information showing a predetermined number of points,

the rental-shop apparatus further comprises a payment unit operable to send to the semiconductor memory, a request to deduct a number of points designated by the user, as a part or all of the payment, when receiving the payment from the user, and

the semiconductor memory deducts the designated number of points from the predetermined number of points according to the request from the rental-shop apparatus, to update the

point information.

17. The rental-shop apparatus of Claim 16,

wherein when receiving the payment from the user, the payment unit generates a number of points in accordance with the payment to be received, and sends to the semiconductor memory, a request to add the generated points, and

the semiconductor memory adds the generated points to the points shown by the point information according to the request from the rental-shop apparatus, to update the point information.

18. The rental-shop apparatus of Claim 14,

wherein another one of the plurality of application functions is a payment function that is used to make the payment for rental from the user to the rental agent, and the application area corresponding to the payment function prestores electric money information showing a predetermined amount of electric money that can be used instead of actual money,

the rental-shop apparatus further comprises a payment unit operable to, when receiving the payment from the user, send to the semiconductor memory, a request for an amount of electric money corresponding to the payment, receive electric money information showing the requested amount of

electric money corresponding to the payment from the semiconductor memory, and internally store the received electric money information, and

the semiconductor memory transmits the electric money information showing the requested amount of electric money corresponding to the payment to the rental-shop apparatus according to the request from the rental-shop apparatus, and deducts the requested amount of electric money corresponding to the payment from the amount of electric money shown by the electric money information stored therein, to update the electric money information.

19. A playback apparatus that plays back digital work whose right of use is rented from a rental agent to a user, the digital work being held by a portable storage medium, comprising:

a reading unit operable to securely read right information relating to a right to use the digital work, from an area of a portable semiconductor memory;

a judgment unit operable to judge whether the digital work is allowed to be used, based on the read right information;

an obtaining unit operable to obtain the digital work from the storage medium when the digital work is allowed to be used; and

a playback unit operable to play back the obtained digital

work.

20. The playback apparatus of Claim 19,

wherein the storage medium holds the digital work by storing therein digital content data that has been generated by encrypting the digital work using an encryption key,

the right information stored in the area of the semiconductor memory includes a decryption key to be used to decrypt the digital content data, the decryption key corresponding to the encryption key,

the reading unit reads the right information including the decryption key, and

when the digital work is allowed to be used, the obtaining unit reads the digital content data from the storage medium and decrypts the digital content data using the decryption key included in the read right information, to generate the digital work.

21. The playback apparatus of Claim 19,

wherein the area of the semiconductor memory stores the right information including playback-limiting information showing a limitation to be imposed on playback of the digital work held by the storage medium,

the reading unit reads the right information including the playback-limiting information, and

the judgment unit judges whether the digital work is allowed to be used, based on the playback-limiting information included in the read right information.

22. The playback apparatus of Claim 21,

wherein the playback-limiting information stored in the area of the semiconductor memory shows a rental-use time limit indicating a time limit until when the rental agent allows the user to use the digital work,

the reading unit reads the right information including the playback-limiting information that shows the rental-use time limit, and

the judgment unit compares the rental-use time limit included in the right information with a present date and time, and judges that the digital work is allowed to be used when the rental-use time limit is on or after the present date and time.

23. The playback apparatus of Claim 21,

wherein the playback-limiting information stored in the area of the semiconductor memory shows a rental-use period during which the rental agent allows the user to use the digital work, the rental-use period starting from a time at which the user firstly plays back the digital work, and

the reading unit reads the right information including

the playback-limiting information that shows the rental-use period, and

the judgment unit compares an elapsed date and time at which the rental-use period elapses from the time at which the user firstly plays back the digital work, with a present date and time, and judges that the digital work is allowed to be used when the elapsed date and time is on or after the present date and time.

24. The playback apparatus of Claim 21,

wherein the playback-limiting information stored in the area of the semiconductor memory shows a number of times the user is allowed to play back the digital work,

the reading unit reads the right information including the playback-limiting information that shows the number of times the user is allowed to play back the digital work, and

the judgment unit counts a number of times the digital work has been played back every time the digital work is played back, and judges that the digital work is allowed to be used only when the counted number of times does not exceed the number of times the user is allowed to play back the digital work included in the right information.

25. The playback apparatus of Claim 19,

wherein the storage medium stores first identification

information identifying the digital work,

the right information stored in the area of the semiconductor memory includes second identification information identifying the digital work,

the reading unit reads the right information including the second identification information, and

the judgment unit compares the first identification information stored in the storage medium and the second identification information included in the read right information, and when the first identification information and the second identification information match, judges that the digital work identified by the first identification information is allowed to be used.

26. The playback apparatus of Claim 25,

wherein the storage medium holds the digital work by storing therein digital content data that has been generated by encrypting the digital work using a content key,

the semiconductor memory further prestores, in the area, a device key unique to the semiconductor memory,

the right information stored in the area of the semiconductor memory includes an encrypted content key that has been generated by encrypting the content key using the device key, and

the semiconductor memory further includes a decryption

unit operable to decrypt the encrypted content key stored in the area using the device key to generate a content key, and output the generated content key, and

when the digital work is allowed to be used, the obtaining unit reads the digital content data from the storage medium, receives the content key from the semiconductor memory, and decrypts the read digital content data using the content key, to generate the digital work.

27. The playback apparatus of Claim 25,

wherein the storage medium holds the digital work by storing therein digital content data that has been generated by encrypting the digital work using a content key, and further stores a disc key unique to the storage medium,

the right information stored in the area of the semiconductor memory includes an encrypted content key that has been generated by encrypting the content key using the disc key,

the semiconductor memory further includes a decryption unit operable to receive the disc key from the storage medium via the playback apparatus, decrypt the encrypted content key stored in the area using the obtained disc key to generate a content key, and output the generated content key, and

when the digital work is allowed to be used, the obtaining unit reads the digital content data from the storage medium,

receives the content key from the semiconductor memory, and decrypts the read digital content data using the received content key, to generate the digital work.

28. The playback apparatus of Claim 19, further comprising

an authentication unit operable to perform mutual authentication with the semiconductor memory,

wherein the reading unit reads the right information when the mutual authentication is successful.

29. The playback apparatus of Claim 19,

wherein the area of the semiconductor memory includes a plurality of application areas being provided in one-to-one correspondence with a plurality of application functions, each application area being provided for securely storing information for the corresponding application function,

one of the plurality of application functions is a rental function of renting the storage medium for use in a storage-medium rental system, and the application area corresponding to the rental function is used to store the right information, and

the reading unit reads the right information from the application area corresponding to the rental function.

30. The playback apparatus of Claim 29,

wherein another one of the plurality of application functions is a payment function that is used to make a payment for rental from the user to the rental agent, and the application area corresponding to the payment function prestores electric ticket information showing electric tickets that can be used to make a payment for playback of the digital work,

the playback apparatus further comprises a request unit operable to send, to the semiconductor memory, a request to deduct electric tickets corresponding to the payment determined in accordance with the playback of the digital work, and

the semiconductor memory further includes a payment unit operable to deduct the electric tickets corresponding to the payment from the electric tickets shown by the electric ticket information stored in the application area, in accordance with the request from the playback apparatus.

31. The playback apparatus of Claim 30, further comprising:

a control unit operable to obtain, before the digital work is played back by the playback unit, electric ticket information showing remaining electric tickets from the semiconductor memory, and judge that the digital work is not allowed to be used and prohibit the playback unit from playing

back the digital work, when the remaining electric tickets are less than the electric tickets corresponding to the payment determined in accordance with the playback of the digital work.

32. The playback apparatus of Claim 31,

wherein the request unit sends to the semiconductor memory, a request to deduct electric tickets corresponding to a payment for playback of one-time, every time the digital work is played back.

33. The playback apparatus of Claim 31,

wherein the request unit sends to the semiconductor memory, a request to deduct electric tickets corresponding to a payment for the playback of the digital work during a predetermined period of time, when the digital work is played back one or more times during the predetermined period of time.

34. A portable semiconductor memory, comprising

a storage unit that has an area for securing storing right information when a rental agent provides a storage medium holding digital work to a user, the right information relating to a right to use the digital work.

35. The semiconductor memory of Claim 34,

wherein the storage medium holds the digital work by storing therein digital content data that has been generated by encrypting the digital work using a content key,

the semiconductor memory further prestores, in the area, a device key unique to the semiconductor memory,

the right information stored in the area of the semiconductor memory includes an encrypted content key that has been generated by encrypting the content key using the device key, and

the semiconductor memory further comprises a decryption unit operable to decrypt the encrypted content key stored in the area using the device key to generate a content key, and output the generated content key.

36. The semiconductor memory of Claim 34,

wherein the storage medium holds the digital work by storing therein digital content data that has been generated by encrypting the digital work using a content key, and further stores a disc key unique to the storage medium,

the right information stored in the area of the semiconductor memory includes an encrypted content key that has been generated by encrypting the content key using the disc key, and

the semiconductor memory further comprises a decryption

unit operable to obtain the disc key from the storage medium via a playback apparatus, decrypt the encrypted content key stored in the area using the obtained disc key to generate a content key, and output the generated content key.

37. The semiconductor memory of Claim 34,

wherein the area of the semiconductor memory includes a plurality of application areas being provided in one-to-one correspondence with a plurality of application functions, each application area being provided for securely storing information for the corresponding application function,

one of the plurality of application functions is a rental function of renting the storage medium for use in a storage-medium rental system, and

the application area corresponding to the rental function is used to store the right information.

38. The semiconductor memory of Claim 37,

wherein another one of the plurality of application functions is a membership card function of identifying a member of a rental shop, and the application area corresponding to the membership card function is used to store a member number that identifies the user.

39. The semiconductor memory of Claim 38,

wherein another one of the plurality of application functions is a bonus provision function of providing, from the rental agent to the user, point information showing points as a bonus in accordance with use of the storage medium, and the application area corresponding to the bonus provision function is used to store point information showing a predetermined number of points that can be used to make a payment for playback of the digital work,

a rental-shop apparatus sends to the semiconductor memory, a request to deduct a number of points designated by the user, as a part or all of the payment, when receiving the payment from the user, and

the semiconductor memory further comprises a payment unit operable to deduct the designated number of points from the predetermined number of points shown by the point information, according to the request from the rental-shop apparatus.

40. The semiconductor memory of Claim 39,

wherein when receiving the payment from the user, the rental-shop apparatus generates point information showing a number of points in accordance with the payment to be received, and outputs the generated point information to the semiconductor memory, and

the semiconductor memory receives the point information,

and additionally writes the received point information into the application area corresponding to the bonus provision function.

41. The semiconductor memory of Claim 37,

wherein another one of the plurality of application functions is a payment function that is used to make the payment for rental from the user to the rental agent, and the application area corresponding to the payment function prestores electric money information showing a predetermined amount of electric money that can be used instead of actual money,

a rental-shop apparatus, when receiving the payment from the user, sends to the semiconductor memory, a request for electric money information showing an amount of electric money corresponding to the payment, receives the electric money information showing the requested amount of electric money corresponding to the payment from the semiconductor memory, and internally stores the received electric money information, and

the semiconductor memory further comprises a payment unit operable to transmit the electric money information showing the requested amount of electric money corresponding to the payment to the rental-shop apparatus according to the request from the rental-shop apparatus, and deduct the

requested amount of electric money corresponding to the payment from the amount of electric money shown by the electric money information stored therein.

42. The semiconductor memory of Claim 37,

wherein another one of the plurality of application functions is a payment function that is used to make a payment for rental from the user to the rental agent, and the application area corresponding to the payment function prestores electric ticket information showing electric tickets that can be used to make a payment for playback of the digital work,

a playback apparatus sends, to the semiconductor memory, a request to deduct electric ticket information showing electric tickets corresponding to the payment determined in accordance with the playback of the digital work, when playing back the digital work, and

the semiconductor memory further includes a payment unit operable to deduct the electric tickets corresponding to the payment from the electric tickets shown by the electric ticket information stored in the application area, in accordance with the request from the playback apparatus.

43. A rental method for use in a rental-shop apparatus that manages rental, from a rental agent to a user, of a right to use digital work held by a portable storage medium,

comprising:

an obtaining step of obtaining medium identification information identifying the storage medium;

a generation step of generating right information relating to the right to use the digital work, based on the obtained medium identification information; and

a writing step of securely writing the generated right information into an area of a portable semiconductor memory.

44. A rental program for use in a computer that manages rental, from a rental agent to a user, of a right to use digital work held by a portable storage medium, comprising:

an obtaining step of obtaining medium identification information identifying the storage medium;

a generation step of generating right information relating to the right to use the digital work, based on the obtained medium identification information; and

a writing step of securely writing the generated right information into an area of a portable semiconductor memory.

45. The rental program of Claim 44, stored in a computer-readable storage medium.

46. A playback method for use in a playback apparatus that plays back digital work whose right of use is rented

from a rental agent to a user, the digital work being held by a portable storage medium, comprising:

a reading step of securely reading right information relating to a right to use the digital work, from an area of a portable semiconductor memory;

a judgment step of judging whether the digital work is allowed to be used, based on the read right information;

an obtaining step of obtaining the digital work from the storage medium when the digital work is allowed to be used; and

a playback step of playing back the obtained digital work.

47. A playback program for use in a computer that plays back digital work whose right of use is rented from a rental agent to a user, the digital work being held by a portable storage medium, comprising:

a reading step of securely reading right information relating to a right to use the digital work, from an area of a portable semiconductor memory;

a judgment step of judging whether the digital work is allowed to be used, based on the read right information;

an obtaining step of obtaining the digital work from the storage medium when the digital work is allowed to be used; and

a playback step of playing back the obtained digital work.

48. The playback program of Claim 47, stored in a computer-readable storage medium.